



UNITED STATES PATENT AND TRADEMARK OFFICE

A
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/073,565	02/11/2002	Cynthia Gayle Eaker		5147

7590 08/19/2005

Cynthia Gayle Eaker
167 Braly Drive
Summerville, SC 29485

EXAMINER

KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 08/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/073,565

Applicant(s)

EAKER, CYNTHIA GAYLE

Examiner

Paula W. Klimach

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 October 2004.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

HL

DETAILED ACTION

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

Claim 1 includes the limitation wherein the improvement whereby said encryption system and method produces ciphertext that varies when a message is coded even if said message is coded many times with the same key. However the specification does not disclose the parts of the system that are used to create this improvement. The examiner assumes that the system is a stream cipher. As disclosed by Schneier (page 198), “Two keystream generators with the same key and the same internal state, will produce the same keystream.” What part of the applicant’s system produces the improvement of producing cipher text that varies when a message is coded even if said message is coded many times with the same key? How is the system used to produce the improved results?

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-19 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in

the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Claim 1 includes the limitation wherein the improvement whereby said encryption system and method produces ciphertext that varies when a message is coded even if said message is coded many times with the same key. However the specification does not describe the parts of the system that are used to create this improvement. The examiner assumes that the system is a stream cipher. As disclosed by Schneier (page 198), "Two keystream generators with the same key and the same internal state, will produce the same keystream." What part of the applicant's system produces the improvement of producing cipher text that varies when a message is coded even if said message is coded many times with the same key? How is the system used to produce the improved results?

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-19 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite in that it fails to point out what is included or excluded by the claim language. This claim is an omnibus type claim. The claim discloses character transformation and transposition accomplished in a myriad of ways. Therefore the applicant has not disclosed the method claimed for transformation and transposition instead the applicant discloses that it is performed in a myriad of ways which would included a large number of unidentified methods.

Claim 11 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Where applicant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The term “asymmetric encryption system” in claim 11 is used by the claim to mean “method of determining a symmetric key from date information”, while the accepted meaning is “public key algorithms; algorithms that are designed so that the key used for encryption is different from the key used for decryption.” The term is indefinite because the specification does not clearly redefine the term.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-9 and 12-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Yanovsky.

In reference to claim 1 the applicant admitted prior art includes an encryption system and method of the type using character transformation and transposition accomplished in myriad ways determined by a key, that is chosen by the user, which determines how said transposition is performed and also determines what characters are transformed into by the use of a digit ring having a prime number of digits which are determined by said key and yields a multitude of unique digit sequences by a variable starting point and variable skip size on said digit ring to harvest digits from said ring to effect said transformation,

Wherein the improvement to the encryption system and method produces ciphertext that varies when a message is coded even if said message is coded many times with the same key.

Yanovsky discloses a method and apparatus for transmitting encrypted messages between two units, by initializing the two units with respect to each other and thereafter transmitting the message between the two units (abstract). Yanovsky discloses the system includes a one way function producing predetermined outputs from known inputs, but not permitting the inputs to be determined from the outputs (column 8 lines 6-17).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to change the output for the same key and input as in Yanovsky. One of ordinary skill in the art would have been motivated to do this because the randomness of the output from the same input would increase the security by decreasing the ability to guess the output from the input.

In reference to claim 2 wherein said ciphertext produced is always all unbroken string of 100 possible characters without spaces or returns in no recognizable order and having characters that vary each time a message is coded even if said message is coded many times with the key.

Yanovsky discloses dividing the input into segments with a segment length of SL_i which is a variable that can be set to 100. The segments include text and therefore include characters without spaces. The characters vary each time a message is coded even if said message is coded may time with the key because of the random number of redundancy bits added in the system of Yanovsky (column 8 lines 26-42).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to set a format of the plaintext as in Yanovsky. One of ordinary skill in the art would have been motivated to do this because it would facilitate the receiver to reconstruct the message in the format agreed upon.

In reference to claims 3 and 16 wherein character transformation is accomplished by message digits being summed with digits determined by said key using addition without carries.

Yanovsky discloses the transformation accomplished by message digits being summed with digits determined by said key using addition without carries (Fig. 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to sum the message with the digits determined by a key using an addition without carries. One of ordinary skill in the art would have been motivated to do this because the addition or the random number (key) will create confusion in the message and therefore the ciphertext output.

In reference to claim 4 wherein said transposition is accomplished by the transformed digit string being reordered to match the order of a sequence of digits that do not repeat and are determined by said key.

Yanovsky discloses a system wherein said transposition is accomplished by the transformed digit string being reordered to match the order of a sequence of digits that do not repeat and are determined by said key (Fig. 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to set a format of the plaintext as in Yanovsky. One of ordinary skill in the art would have been motivated to do this because it would facilitate the receiver to reconstruct the message in the format agreed upon.

In reference to claim 5 wherein information is automatically coded and decoded using appropriate keys once communication has been established.

Yanovsky discloses a system wherein information is automatically coded and decoded using appropriate keys once communication has been established (Fig. 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to code and decode using the appropriate keys as in Yanovsky. One of ordinary skill in the art would have been motivated to do this because the one way function requires the correct key for in order to decode the message correctly.

In reference claim 6 wherein two numbers are chosen at random to determine said starting position on said digit ring and said skip size around said digit ring to harvest digits for said character transformation.

Yanovsky discloses a system wherein two numbers are chosen at random to determine said starting position on said digit ring and said skip size around said digit ring to harvest digits for said character transformation (Fig. 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to code and decode using the appropriate keys as in Yanovsky. One of ordinary skill in the art would have been motivated to do this because the one way function requires the correct key for in order to decode the message correctly.

In reference to claim 7 wherein said key made from a small amount of text is used to make a multitude of unique digit sequences composed of unique numbers that do not repeat that are used to shuffle digits to achieve said transposition and said key is also expanded to make a large prime string of digits that is relatively random and used as said digit ring to harvest digits used in said transformation.

Yanovsky discloses a system wherein said key made from a small amount of text is used to make a multitude of unique digit sequences composed of unique numbers that do not repeat that are used to shuffle digits to achieve said transposition and said key is also expanded to make a large prime string of digits that is relatively random and used as said digit ring to harvest digits used in said transformation (Fig. 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to code and decode using the appropriate keys as in Yanovsky. One of ordinary skill in the art would have been motivated to do this because the one way function requires the correct key for in order to decode the message correctly.

In reference to claim 8 wherein the variable digits that determine said starting point on said digit ring and skip size around said digit ring and the variable digits used in said transformation and transposition are mixed into the digit sequence that becomes ciphertext.

Yanovsky discloses a system wherein the variable digits that determine said starting point on said digit ring and skip size around said digit ring and the variable digits used in said transformation and transposition are mixed into the digit sequence that becomes ciphertext (Fig. 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to code and decode using the appropriate keys as in Yanovsky. One of ordinary skill in the art would have been motivated to do this because the one way function requires the correct key for in order to decode the message correctly.

In reference to claim 9 wherein the system and method used to code the message is determined by at least one cipher character that is mixed into the ciphertext.

Yanovsky discloses a system used to code the message is determined by at least one cipher character that is mixed into the ciphertext (Fig. 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to code and decode using the appropriate keys as in Yanovsky. One of ordinary skill in the art would have been motivated to do this because the one way function requires the correct key for in order to decode the message correctly.

In reference to claim 12 further including a variation of the system and method that replaces character patterns often seen in plaintext messages with a smaller unique character sequence before the standard encryption process resulting in compression of the ciphertext.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to replace character patterns often seen in plaintext messages with a smaller unique character. One of ordinary skill in the art would have been motivated to do this because

it would reduce the probability of repetition of the output from the input and therefore making cryptanalysis easier

In reference to claim 13 further including variation of the system and method that codes and decodes audio and digital information.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to code and decode audio and digital information. One of ordinary skill in the art would have been motivated to do this because it is the information most often transmitted, most easily reproduced and therefore the information that is most desirable to secure.

In reference to claims 14 and 19 further including a variation using a high quality random number generator used to generate title digits for said start and said skip numbers and other random numbers used in said encryption system and method.

Yanovsky discloses a system including a variation using a high quality random number generator used to generate title digits for said start and said skip numbers and other random numbers used in said encryption system and method (Fig. 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a quality random number generator used to generate title digits for said start and said skip numbers and other random numbers used in said encryption system and method. One of ordinary skill in the art would have been motivated to do this because random numbers make strong keys and therefore increase the security of the system.

In reference to claim 15, further including a variation with said start and said skip numbers that are not determined at random but by the number of seconds that have elapsed since

the new year began accurate to a fraction of a second and summed using standard addition with numbers from digits found in the unique digit sequences determined by said key.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use timestamp. One of ordinary skill in the art would have been motivated to do this because timestamp reduce the probability of reuse of secret data.

In reference to claim 17 further including a variation that relies upon high quality transformation that renders transposition unnecessary for encryption strength.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a variation that relies upon high quality transformation that renders transposition unnecessary for encryption strength. One of ordinary skill in the art would have been motivated to do this because it would decrease the number of operations required.

In reference to claim 18 further including a variation of the system and method that provides means for coding of coded messages by first converting all cipher characters into characters that are valid for coding.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to set a format of the plaintext as in Yanovsky. One of ordinary skill in the art would have been motivated to do this because it would facilitate the receiver to reconstruct the message in the format agreed upon.

Claims 10-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art and further in view of Yanovsky as applied to claim 1 above, and further in view of Schneier.

In reference to claim 10 further including enhanced end user security by corrupting and or removing unique number sequences determined by said key when said encryption system and method is not in use.

Applicant admitted prior art and Yanovsky do not teach removing unique number sequences determined by the key.

Schneier disclose destroying keys that have been used (page 15)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to destroy keys that have been already used. One of ordinary skill in the art would have been motivated to do this because this would prevent them from being used again by mistake and therefore making the system more secure.

In reference to claim 11 further including a system and method variation that makes said encryption system and method asymmetric by using the number of seconds elapse since the year began and digits that vary in the year positions to determine start and side numbers making repetition of digit sequences used for character transformation statistically impossible for up to 100 years using said system and method variation.

Applicant admitted prior art and Yanovsky do not teach using a timestamp as part of key generation

Schneier teaches using a timestamp as part of key generation (page 175).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use date and time for key generation. One of ordinary skill in the art would have been motivated to do this because it does not generate easy to remember keys.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Yahovsky

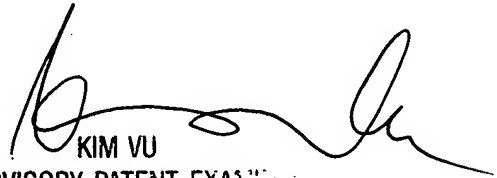
5,703,948

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Wednesday, August 10, 2005


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2135